System Protection Profile for Industrial Control Systems

Version 0.88

December 3, 2003

Table of Contents

1 Introduction

The System Protection Profile (SPP) Introduction provides a coherent, consistent and sufficiently complete high-level description of the system and provides an accurate and correct set of identifying information for the SPP as a document.

1.1 System Protection Profile Identification

Title: System Protection Profile for Industrial Control Systems, Version 0.88, December 3, 2003

Registration:

Keywords: industrial control system,

1.2 System Protection Profile Overview

The System Protection Profile for Industrial Control Systems (SPP-ICS) specifies the integrated set of security requirements for industrial control systems. The integrated set of requirements includes requirements for operating policies and procedures, requirements for information technology based system components, requirements for interfaces and interoperability between system components, and requirements for the physical environment and protection of the system.

Because the SPP-ICS represents an integrated view of the requirements, special consideration is given to decomposition of security functionality and assignment of specific security functions to sub-systems or components of the overall integrated system. Likewise, the recomposition or composability of the security functionality is also considered. The goal of this aspect of analysis and design is to define security requirements for subsystems or system components at the lowest possible level while at the same time retaining the required level of assurance and security functionality for the integrated system as a whole.

As shown in Figure 1 an industrial control system consists of classes of components for the direct control of a process (the controller(s), actuators and sensors) a human machine interface and capabilities for remote diagnostics and maintenance.

This system protection profile is written for a generic industrial control system as a high-level statement of requirements. It provides a starting point for more specific and detailed statements of requirements for industrial control systems focused on a specific industry, company, or component.

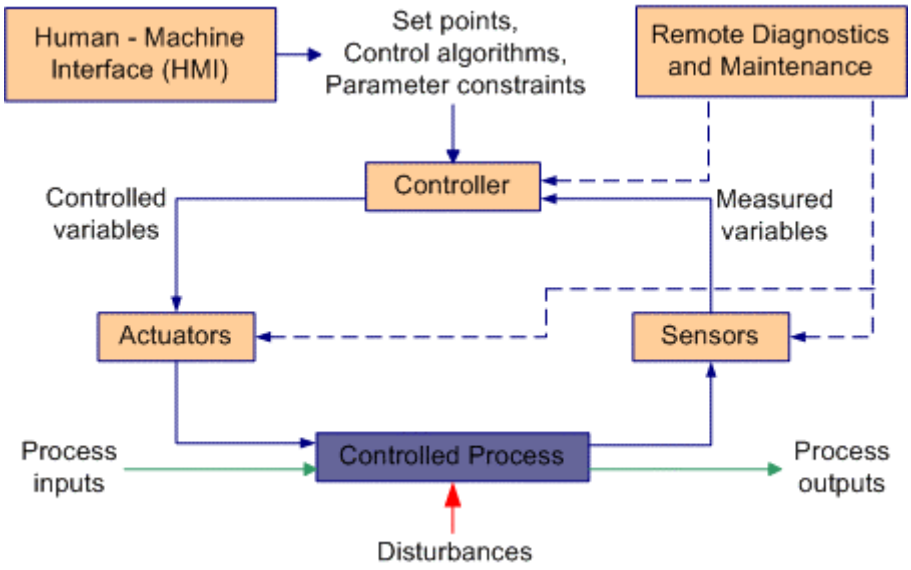


Figure 1 Fundamental industrial control system components

2 System Target of Evaluation Description

This section describes the security subsystem of the industrial control system. The security subsystem includes both the information technology based components and the non-information technology based elements implemented via policies and operating procedures. Particular attention is given to the interaction and dependencies between the security subsystem and the overall industrial control system.

The System Target of Evaluation (STOE) is depicted graphically in Figure 2. The STOE consists of the security services and procedures, both automated and manual, which are designed to meet the security objectives defined to counter threats to the ICS. Note that the corporate intranet is in the external environment of the STOE.

Boxes with bold red borders depict the primary system security functions. These functions are: user authentication services (including user access control), physical access control, boundary protection, and data / device authentication. User authentication services control access to process control related computer systems including the human machine interface (HMI) and remote diagnostics and maintenance. In addition, user authentication is used by the physical access control system to authenticate personnel for physical access. Data / device authentication is shown as a separate function to emphasize the need for data and command signal authentication.

The blue lines from actuator to controlled process and from controlled process to sensor indicate that these are physical connections representing the direct interactions that take place. The rest of the diagram depicts logical connections.

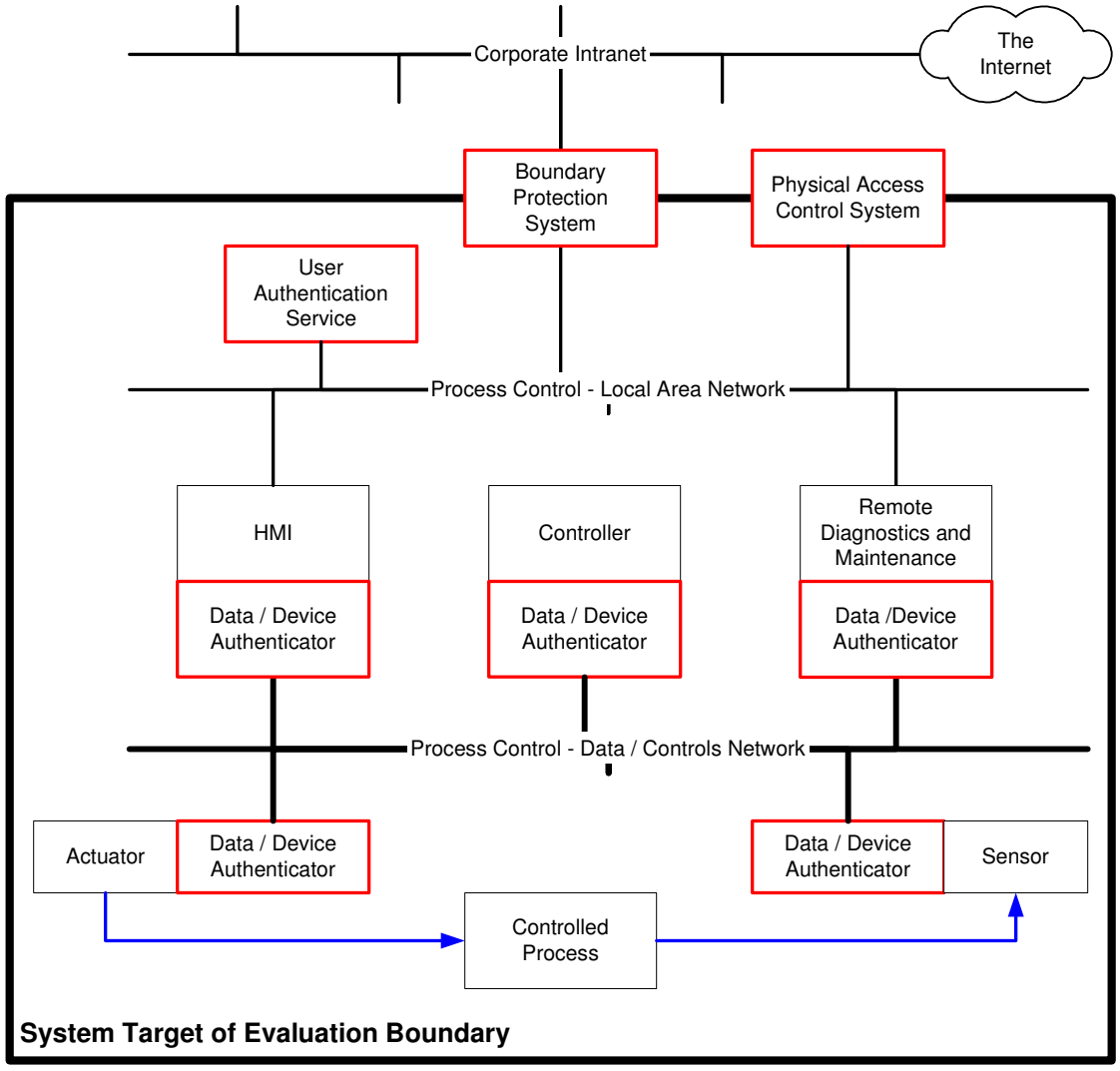


Figure 2 Graphical depiction of System Target of Evaluation

3 STOE Security Environment

This section provides a description of the security problem addressed by the target of evaluation. The problem is stated in terms of the threats that will be countered by the system and the organizational security policies that support and govern the use of the system.

3.1 Organizational Security Policies

This section describes the Overarching Organizational Security Policies (OOSPs) that define the broader context of the organization which support and govern the use of a system. These will form part of the basis for deriving the actual organizational security policies (OSPs) to be included as part of a specific system TOE.

The scope of organizational security policy includes both the organizational security policies of the organization that has responsibility for operating the industrial control system as well as those for any external organizations that the industrial control system interacts with.

3.2 Assumptions

This section documents any security relevant assumptions.

3.3 System Risk Assessment

This section describes the approach that has been used to characterize the security related risks for an industrial control system and the means for determining residual risk remaining after countermeasures have been implemented.

The SPP-ICS describes the security requirements at a high level of abstraction appropriate to the generic nature of the industrial control system as represented in Figure 1. Each of the critical assets identified below represents a class of assets and the threats identified in section 3.5 represent classes of threats against those assets. Within the SPP-ICS a general framework for risk management is established that will be elaborated in subsequent SPPs developed for specific classes of industrial control systems, for example, Supervisory Control and Data Acquisition (SCADA) systems.

3.4 Critical assets

This section identifies the critical information and other assets associated with the generic industrial control system.

From Figure 1 and **Error! Reference source not found.** the following critical assets can be identified:

- Actuators
- Sensors
- Controllers
- Human – Machine Interfaces (HMIs)
- Remote Diagnostics and Maintenance
- Communications Infrastructure
- The Controlled Process (including the inputs and outputs to the process)
- The process control information being collected by, processed by, stored on and transmitted to or from the components that constitute the process control network
- The process control business or financial information being created by, processed by, stored on and transmitted to or from the components that constitute the process control network

3.5 Threat areas of concern for critical assets

This section documents the threat areas of concern for the critical assets.

Threats to critical assets may be summarized in a table of "threat properties for areas of concern". Using this approach threats are characterized with the following parameters:[1]

- Asset – something of value to the organization (information in electronic or physical form, information systems, a group of people with unique expertise)
- Actor – who or what may attempt to violate the security policy (confidentiality, integrity, availability) pertaining to an asset. Actors can be from inside or outside the organization.
- Motive (optional) – indication of whether the actor's intentions are deliberate or accidental
- Access (optional) – how the asset will be accessed by the actor (network access or physical access)
- Outcome – the immediate result of violating the security policy pertaining to an asset (disclosure, modification, destruction, loss, interruption)

For the SPP-ICS the threat areas of concern are broadly stated for classes of assets and are defined at a high level of abstraction. The threat areas of concern are documented in Table 3-1.

Table 3-1 Threat areas of concern for Industrial Control Systems

Areas of Concern	Threat Properties
1. Loss of control system integrity through deliberate alteration of control algorithms, component parameters, etc. by an outsider with hostile intent	• Asset: ICS configuration • Actor: Outsider • Motive: deliberate • Access: network • Outcome: disruption, damage or loss
2. Loss of control system integrity through deliberate alteration of control algorithms, component parameters, etc. by a disgruntled former employee, contractor, etc.	• Asset: ICS configuration • Actor: Former insider (e.g., striking worker) • Motive: deliberate • Access: network or physical • Outcome: disruption, damage or loss
3. Loss of control system integrity through deliberate alteration of control algorithms, component parameters, etc. by a disgruntled employee	• Asset: ICS configuration • Actor: Insider • Motive: deliberate • Access: network or physical • Outcome: disruption, damage or loss
4. Loss of control system integrity	• Asset: ICS configuration

[1] Alberts, Christopher and Audrey Dorofee. "Octave[SM] Threat Profiles" Available for download from http://www.cert.org/archive/pdf/OCTAVEthreatProfiles.pdf

Areas of Concern	Threat Properties
through accidental alteration of control algorithms, component parameters, etc.	• Actor: insider • Motive: accidental • Access: network or physical • Outcome: disruption, damage or loss
5. Loss of control system availability through deliberate actions of an outsider resulting in shutdown of process	• Asset: ICS • Actor: Outsider • Motive: deliberate • Access: network • Outcome: ICS unavailable
6. Loss of control system availability through deliberate actions of a former insider resulting in shutdown of process	• Asset: ICS • Actor: Former insider • Motive: deliberate • Access: physical or network • Outcome: ICS unavailable
7. Loss of control system availability through deliberate actions of a disgruntled insider resulting in shutdown of process	• Asset: ICS • Actor: Insider • Motive: deliberate • Access: network, physical • Outcome: ICS unavailable
8. Loss of control system availability through accidental actions of an insider resulting in shutdown of process	• Asset: ICS component • Actor: Insider • Motive: accidental • Access: network, physical • Outcome: ICS unavailable
9. Loss of control system availability through an act of nature resulting in shutdown of process	• Asset: ICS component • Actor: Act of nature • Motive: accidental • Access: physical • Outcome: ICS unavailable
10. Unauthorized control of process by an outsider through introduction of false control signals	• Asset: Controlled process • Actor: Outsider • Motive: deliberate • Access: network • Outcome: loss of control of process
11. False information on HMI (operator) displays to mask unauthorized control of process or other activities	• Asset: HMI • Actor: Outsider • Motive: deliberate • Access: network • Outcome: modification - loss of integrity for process data
12. Corruption of business or financial data transferred from ICS to business systems	• Asset: Business or financial data from ICS

Areas of Concern	Threat Properties
	• Actor: Insider • Motive: deliberate • Access: network • Outcome: modification
13. Corruption of business or financial data transferred from ICS to business systems	• Asset: Business or financial data from ICS • Actor: Outsider • Motive: deliberate • Access: network • Outcome: modification

3.6 Risk Assessment and Impact Analysis

This section documents the analysis of risk and impact to critical assets if a threat is successfully carried out.

It is the responsibility of the system owner(s) to assess the operational environment, to determine the assets that need protecting, and to determine the level to which the organization is willing to take to assure that the assets will not be lost or compromised. This should be documented to the detail necessary to understand that the security counter-measures effectively addresses the risk tolerance threshold. Because the operational environment of the system is fully known, the risk assessment can be fully completed.

3.6.1 Risk Management

Risk management is the process of assessing risks in the operational environment and making accountable decisions about how risks are to be handled. Risk is expressed using three basic sub-expressions:

- An identified business asset (with an attributed value);
- An attack (which exploits a security weakness or failure);
- An attacker or Actor (an unauthorised user of the business asset).

Once a risk has been identified, there are essentially four ways it can be handled:

- Accept the risk, and acknowledge liability for the cost should the risk be realised;
- Transfer the risk, and the liability for the cost, to another party;
- Abandon the activity which causes the risk;
- Limit the risk to an acceptable tolerance (by the implementation of counter-measures to reduce the likelihood and/or the impact of the risk), and acknowledge liability for the remaining cost should the limited risk be realised.

The expression used to describe a risk reduced to an acceptable tolerance, i.e. reduced to a level acceptable to the system owner(s), is the term Acceptable Risk.

3.6.2 Risk Assessment

Risk assessment is the first step in any risk management approach. Risk assessment is the systematic consideration of the risks in the operational environment in order to determine the appropriate way in which a risk is to be handled (i.e. accept, transfer, abandon or limit). The risk assessment is based on an analysis of the:

- Probability of a risk being realised;
- Impact (harm or otherwise) to the business asset that would likely result from the risk being realised.

The process of risk assessment generally needs to be performed iteratively in order to address the required combinations of systems, sub-systems, components or services and the areas of organisations in which they may be used or deployed.

3.6.3 Limit Risk through Security counter-measures

Risks that cannot be accepted, transferred or the activity abandoned must be limited to a level of tolerance, acceptable to the system owner(s), by the implementation of security counter-measures drawn from the following categories:

- Physical;
- Procedural;
- Personnel;
- Technical.

The process of systematically assessing risks and selecting security counter-measures generally needs to be performed a number of times to address different combinations of systems, sub-systems, components or services and the areas of organisations in which they may be used or deployed.

3.6.4 Periodic Review of Risk / Impact Analysis

It is the responsibility of the system owner(s) to periodically review their assessment of the operational environment, to determine whether:

- There are changes to business assets;
- There are new risks, or changes to risks to assets;
- The existing counter-measures are still appropriate.

Risk assessment is used to determine the extent of the potential threat and the risk associated with a system throughout its' lifecycle. The output of the risk assessment helps

the subsequent identification of the appropriate security counter-measures for the reporting, mitigation or elimination of risk, i.e. how it should be managed.

Risk is a combination of the likelihood that a particular vulnerability in a system will be either intentionally or unintentionally exploited by a particular threat agent or Actor and the potential impact on the system operations, assets or individuals should the exploitation occur.

<Editor Note> Details of the analysis of the risk goes here …

4 Security Objectives

This section provides a coherent, consistent and sufficiently complete high-level description of the solution to the security problem definition stated in section 3. The statement of solution has complete traceability between the security objectives and all aspects of the statement of the security environment. This provides the detailed support for the risk / impact analysis in section 3.6.

The SPP objectives provide the highest-level statement of strategy and philosophy for countering the defined threats, for enforcing the defined organizational security policies and consistent within the bounds of the stated assumptions.

4.1 Security Objectives for the STOE

This section clearly states the security objectives for the STOE and traces them back to aspects of identified threats that will be countered by the STOE.

4.1.1 Objective 1: Boundary protection

Area(s) of concern addressed: 1,2,5,6,10,11,13

O1.1 The STOE must provide protection at the physical network boundaries of the ICS to prevent access to the process control network by unauthorized users.

O1.2 The STOE must provide protection for the physical environment boundaries of the ICS to prevent unauthorized physical access to the ICS and the process plant.

4.1.2 Objective 2: User authentication

Area(s) of concern addressed: 1,2,3,4,5,6,7,8,10,11,12,13

O2.1 The STOE must provide for authentication of ICS users to prevent unauthorized network access to the process control network and the process control devices.

O2.2 The STOE must provide for authentication of people for physical access to the physically protected area to prevent unauthorized physical access to the ICS and the process plant.

O2.3 The STOE shall establish management and operating procedures for revoking authentication credentials for any inactive users (e.g., former employees, former contractors, users who are on strike, etc.) on a timely basis.

4.1.3 Objective 3: Device authentication

Area(s) of concern addressed: 1,2,3,4,5,6,7,8

O3.1 The STOE must provide for authentication of ICS components and systems to help assure the legitimacy of control signals.

4.1.4 Objective 4: System configuration data backup

Area(s) of concern addressed: 1,2,3,4,5,6,7,8,9

O4.1 The STOE must include provisions for ICS data and control information (including executable software and control data) to assure the ability for timely recovery to an operating state if the ICS is compromised or damaged. The data backup procedures should follow industry best practices including (but not limited to) secondary storage locations, testing of recovery procedures, and a back up interval either driven by configuration changes or a specified time interval or a combination of both.

4.1.5 Objective 5: Data authentication

Area(s) of concern addressed: 10,11,12,13

O5.1 The STOE shall authenticate configuration change commands such that configuration (control algorithms, set points, limit points, etc.) cannot be changed unless the integrity of the command can be positively established.

O5.2 The STOE shall authenticate financial or other business critical information sent from the STOE to external systems with a minimum of a time stamped digital signature.

4.1.6 Objective 6: Password management

Area(s) of concern addressed: 1,2,5,6,10,13

O6.1 The STOE shall establish password management procedures that include the use of medium strength passwords, that require changing passwords on an interval no less than 1 year, that require revocation of passwords for inactive users (e.g., former employees, former contractors, users who are on strike, etc.) on a timely basis.

4.2 Security Objectives for the environment

This section clearly states aspects of identified threats that will not be completely countered by the STOE and/or broader organizational security policies or assumptions note completely met by the STOE.

4.2.1 Backup Power

OE1.1 Emergency backup power will be available to the ICS with sufficient capacity to permit safe and recoverable shutdown of the process if external power is lost.

< Editor Note: Additional items TBD >

4.3 Security objective coverage for threat areas of concern

This section demonstrates the degree to which the security objectives counter the threats as defined in the threat areas of concern.

		Threat Area of Concern												
Security Objective		1	2	3	4	5	6	7	8	9	10	11	12	13
	1	X	X			X	X				X	X		X
	2	X	X	X	X	X	X	X	X		X	X	X	X
	3	X	X	X	X	X	X	X	X					
	4	X	X	X	X	X	X	X	X	X				
	5										X	X	X	X
	6	X	X			X	X				X			X

Table 4-1 Security objective coverage of threat areas of concern

5 Security Requirements

This section contains complete and concise requirements for the system TOE. This includes system security functional requirements and system security assurance requirements. The requirements are primarily stated as logical requirements and cover information technology related requirements, requirements for system security policies and system security related operating procedures, and integration requirements addressing interfaces and interoperability between security system components.

5.1 IT Security Requirements

5.1.1 Logon Controls:

FIA_UID.1 Timing of identification
Hierarchical to: No other components.

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: No dependencies

FIA_UAU.1 Timing of authentication
Hierarchical to: No other components.

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies: **FIA_UID.1 Timing of identification**

FIA_UAU.2 User authentication before any action
Hierarchical to: FIA_UAU.1

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing **any other TSF-mediated actions** on behalf of that user.
Dependencies: **FIA_UID.1 Timing of identification**

FIA_AFL.1 Authentication failure handling
Hierarchical to: No other components.

FIA_AFL.1.1 The TSF shall detect when [assignment: *number*] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [assignment: *list of actions*].
Dependencies: **FIA_UAU.1 Timing of authentication**

FTP_TRP.1 Trusted path
Hierarchical to: No other components.

FTP_TRP.1.1 The TSF shall provide a communication path between itself and [selection: *remote, local*] users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from modification or disclosure.

FTP_TRP.1.2 The TSF shall permit [selection: *the TSF, local users, remote users*] to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [selection: *initial user authentication*, [assignment: *other services for which trusted path is required*].
Dependencies: No dependencies

FTA_TSE.1 TOE session establishment
Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [assignment: *attributes*].
Dependencies: No dependencies

5.1.2 Password Selection

FIA_SOS.1 Verification of *passwords*
Hierarchical to: No other components.
FIA_SOS.1.1 The TSF shall provide a mechanism to verify that *passwords* meet [assignment: *a defined quality metric*].
Dependencies: No dependencies

FIA_SOS.2 TSF Generation of *passwords*
Hierarchical to: No other components.
FIA_SOS.2.1 The TSF shall provide a mechanism to generate *passwords* that meet [assignment: *a defined quality metric*].
FIA_SOS.2.2 The TSF shall be able to enforce the use of TSF generated *passwords* for [assignment: *list of TSF functions*].
Dependencies: No dependencies

FMT_SAE.1 Time-limited authorisation
Hierarchical to: No other components.
FMT_SAE.1.1 The TSF shall restrict the capability to specify an expiration time for [assignment: *list of security attributes for which expiration is to be supported*] to [assignment: *the authorised identified roles*].
FMT_SAE.1.2 For each of these security attributes, the TSF shall be able to [assignment: *list of actions to be taken for each security attribute*] after the expiration time for the indicated security attribute has passed.
Dependencies: **FMT_SMR.1 Security roles**
FPT_STM.1 Reliable time stamps

5.1.3 Authentication Data Protection

FIA_UAU.7 Protected authentication feedback
Hierarchical to: No other components.
FIA_UAU.7.1 The TSF shall provide only [assignment: *list of feedback*] to the user while the authentication is in progress.
Dependencies: **FIA_UAU.1 Timing of authentication**
(For passwords)

FMT_MTD.1Management of TSF data
Hierarchical to: No other components.
FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].
Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FPT_RPL.1 Replay detection
Hierarchical to: No other components.
FPT_RPL.1.1 The TSF shall detect replay for the following entities: [assignment: *list of identified entities*].
FPT_RPL.1.2 The TSF shall perform [assignment: *list of specific actions*] when replay is detected.
Dependencies: No dependencies

5.1.4 Replay / Reuse

FIA_UAU.3 Unforgeable authentication
Hierarchical to: No other components.
FIA_UAU.3.1 The TSF shall [selection: *detect, prevent*] use of authentication data that has been forged by any user of the TSF.
FIA_UAU.3.2 The TSF shall [selection: *detect, prevent*] use of authentication data that has been copied from any other user of the TSF.
Dependencies: No dependencies
FIA_UAU.4 Single-use authentication mechanisms
Hierarchical to: No other components.
FIA_UAU.4.1 The TSF shall prevent reuse of authentication data related to [assignment: *identified authentication mechanism*(s)].
Dependencies: No dependencies
---These are targeted to preventing replay attacks from captured control signals---

5.1.5 Session Suspension

FTA_SSL.1 TSF-initiated session locking
Hierarchical to: No other components.
FTA_SSL.1.1 The TSF shall lock an interactive session after [assignment: *time interval of user inactivity*] by:
a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.
FTA_SSL.1.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].
Dependencies: **FIA_UAU.1 Timing of authentication**

FTA_SSL.2 User-initiated locking

Hierarchical to: No other components.

FTA_SSL.2.1 The TSF shall allow user-initiated locking of the user's own interactive session,
by:
a) clearing or overwriting display devices, making the current contents unreadable;
b) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The TSF shall require the following events to occur prior to unlocking the session: [assignment: *events to occur*].

Dependencies: **FIA_UAU.1 Timing of authentication**

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components.

FTA_SSL.3.1 The TSF shall terminate an interactive session after a [assignment: *time interval of user inactivity*].

Dependencies: No dependencies

5.1.6 User Accounts and Profiles

FMT_MTD.1Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

(User accounts and User profiles)

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [assignment: *list of security attributes*].

Dependencies: No dependencies

(Definition of user security attributes contained in a user profile)

5.1.7 Role based access control

FDP_ACC.1 Subset access control

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects*, *objects, and operations among subjects and objects covered by the SFP*].

Dependencies: **FDP_ACF.1 Security attribute based access control**

FDP_ACC.2 Complete access control

Hierarchical to: FDP_ACC.1

FDP_ACC.2.1 The TSF shall enforce the [assignment: *access control SFP*] on [assignment: *list of subjects and objects*] **and all operations among subjects and objects covered by the SFP.**

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject in the TSC and any object within the TSC are covered by an access control SFP.

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes*, *named groups of security attributes*].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: *rules governing access among controlled subjects and controlled objects using controlled operations on controlled objects*].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [assignment: *rules, based on security attributes, that explicitly authorise access of subjects to objects*].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [assignment: *rules, based on security attributes, that explicitly deny access of subjects to objects*].

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles [assignment: *the authorised identified roles*].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Dependencies: **FIA_UID.1 Timing of identification**

FMT_SMR.2 Restrictions on security roles

Hierarchical to: **FMT_SMR.1**

FMT_SMR.2.1 The TSF shall maintain the roles: [assignment: *the authorised identified roles*].

FMT_SMR.2.2 The TSF shall be able to associate users with roles.

FMT_SMR.2.3 The TSF shall ensure that the conditions [assignment: *a single user account is not assigned the two different roles associated with a two-man rule*] are satisfied.

Dependencies: **FIA_UID.1 Timing of identification**

Application Note: FDP_ACF.1 may be used to specify that particular operations require two distinct roles to authorize the action. FMT_SMR.2.3 can ensure that a user account cannot be assigned to both roles (as used above). If there is more than one situation requiring implementation of a two-man rule the combination should be iterated for each set of roles.

5.1.8 Controls on RBAC Attributes

FMT_MSA.1 Management of security attributes
Hierarchical to: No other components.
FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].
Dependencies: **[FDP_ACC.1 Subset access control or**
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

5.1.9 Firewall access control

FDP_IFC.1 Subset information flow control
Hierarchical to: No other components.
FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects*, *information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].
Dependencies: **FDP_IFF.1 Simple security attributes**
FDP_IFC.2 Complete information flow control
Hierarchical to: FDP_IFC.1
FDP_IFC.2.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects* and *information*] and **all operations that cause that information to flow to and from subjects covered by the SFP.**
FDP_IFC.2.2 The TSF shall ensure that all operations that cause any information in the TSC to flow to and from any subject in the TSC are covered by an information flow control SFP.
Dependencies: **FDP_IFF.1 Simple security attributes**

FDP_IFF.1 Simple security attributes
Hierarchical to: No other components.
FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *the minimum number and type of security attributes*].
FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

[assignment: ***for each operation, the security attribute-based relationship that must hold between subject and information security attributes*****].**

FDP_IFF.1.3 The TSF shall enforce the [assignment: ***additional information flow control SFP rules*****].**

FDP_IFF.1.4 The TSF shall provide the following [assignment: ***list of additional SFP capabilities*****].**

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: ***rules, based on security attributes, that explicitly authorize information flows*****].**

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: [assignment: ***rules, based on security attributes, that explicitly deny information flows*****].**

Dependencies: **FDP_IFC.1 Subset information flow control**

FMT_MSA.3 Static attribute initialisation

5.1.10 Audit events

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the [selection: ***minimum, basic, detailed, not specified*****] level of audit; and**

c) [assignment: ***other specifically defined auditable events*****].**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: ***other audit relevant information*****]**

Dependencies: **FPT_STM.1 Reliable time stamps**

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: **FAU_GEN.1 Audit data generation**
FIA_UID.1 Timing of identification

FMT_MTD.1Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear*, [assignment: *other operations*]] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].
Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

FAU_SEL.1 Selective audit
Hierarchical to: No other components.
FAU_SEL.1.1 The TSF shall be able to include or exclude auditable events from the set of audited events based on the following attributes:
a) [selection: *object identity, user identity, subject identity, host identity, event type*]
b) [assignment: *list of additional attributes that audit selectivity is based upon*].
Dependencies: **FAU_GEN.1 Audit data generation**
FMT_MTD.1 Management of TSF data

5.1.11 Intrusion detection and response

FAU_ARP.1 Security alarms
Hierarchical to: No other components.
FAU_ARP.1.1 The TSF shall take [assignment: *list of the least disruptive actions*] upon detection of a potential security violation.
Dependencies: **FAU_SAA.1 Potential violation analysis**

FAU_SAA.1 Potential violation analysis
Hierarchical to: No other components.
FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.
FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:
a) Accumulation or combination of [assignment: *subset of defined auditable events*] known to indicate a potential security violation;
b) [assignment: *any other rules*].
Dependencies: **FAU_GEN.1 Audit data generation**

FAU_SAA.2 Profile based anomaly detection
Hierarchical to: FAU_SAA.1
FAU_SAA.2.1 The TSF shall be able to maintain profiles of system usage, where an individual profile represents the historical patterns of usage performed by the member(s) of [assignment: *the profile target group*].
FAU_SAA.2.2 The TSF shall be able to maintain a suspicion rating associated with each user whose activity is recorded in a profile, where the suspicion rating represents the degree to which the user's current activity is found inconsistent with the established patterns of usage represented in the profile.

FAU_SAA.2.3 The TSF shall be able to indicate an imminent violation of the TSP when a user's suspicion rating exceeds the following threshold conditions [assignment: *conditions under which anomalous activity is reported by the TSF*].

Dependencies: **FIA_UID.1 Timing of identification**

FAU_SAA.3 Simple attack heuristics

Hierarchical to: FAU_SAA.1

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events [assignment: *a subset of system events*] that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

Dependencies: No dependencies

FAU_SAA.4 Complex attack heuristics

Hierarchical to: FAU_SAA.3

FAU_SAA.4.1 The TSF shall be able to maintain an internal representation of the **following event sequences of known intrusion scenarios [assignment: *list of sequences of system events whose occurrence are representative of known penetration scenarios*] and** the following signature events [assignment: *a subset of system events*] that may indicate a potential violation of the TSP.

FAU_SAA.4.2 The TSF shall be able to compare the signature events **and event sequences** against the record of system activity discernible from an examination of [assignment: *the information to be used to determine system activity*].

FAU_SAA.4.3 The TSF shall be able to indicate an imminent violation of the TSP when **system activity** is found to match a signature event **or event sequence** that indicates a potential violation of the TSP.

Dependencies: No dependencies

5.1.12 Audit trail protection

FAU_STG.1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG.1.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records.

Dependencies: **FAU_GEN.1 Audit data generation**

FAU_STG.2 Guarantees of audit data availability

Hierarchical to: FAU_STG.1

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to [selection: *prevent, detect*] modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that [assignment: *metric for saving audit records*] audit records will be maintained when the following conditions occur: [selection: *audit storage exhaustion, failure, attack*].

Dependencies: FAU_GEN.1 Audit data generation

FAU_STG.3 Action in case of possible audit data loss

Hierarchical to: No other components.

FAU_STG.3.1 The TSF shall take [assignment: *actions to be taken in case of possible audit storage failure*] if the audit trail exceeds [assignment: *pre-defined limit*].

Dependencies: FAU_STG.1 Protected audit trail storage

FAU_STG.4 Prevention of audit data loss

Hierarchical to: FAU_STG.3

FAU_STG.4.1 The TSF shall [selection: *'ignore auditable events', 'prevent auditable events, except those taken by the authorised user with special rights', 'overwrite the oldest stored audit records'*] and [assignment: *other actions to be taken in case of audit storage failure*] if the audit trail is full.

Dependencies: FAU_STG.1 Protected audit trail storage

5.1.13 Audit trail analysis / review

FAU_SAR.1 Audit review

120 This component will provide authorised users the capability to obtain and interpret the information. In case of human users this information needs to be in a human understandable presentation. In case of external IT entities the information needs to be unambiguously represented in an electronic fashion.

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide [assignment: *authorised users*] with the capability to read [assignment: *list of audit information*] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

Dependencies: **FAU_GEN.1 Audit data generation**

FAU_SAR.2 Restricted audit review

Hierarchical to: No other components.

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

Dependencies: **FAU_SAR.1 Audit review**

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components.

FAU_SAR.3.1 The TSF shall provide the ability to perform [selection: *searches, sorting, ordering*] of audit data based on [assignment: *criteria with logical relations*].

Dependencies: **FAU_SAR.1 Audit review**

5.1.14 TOE Integrity

FPT_PHP.1 Passive detection of physical attack

Hierarchical to: No other components.

FPT_PHP.1.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.1.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

Dependencies: **FMT_MOF.1 Management of security functions behaviour**

FPT_PHP.2 Notification of physical attack

Hierarchical to: FPT_PHP.1

FPT_PHP.2.1 The TSF shall provide unambiguous detection of physical tampering that might compromise the TSF.

FPT_PHP.2.2 The TSF shall provide the capability to determine whether physical tampering with the TSF's devices or TSF's elements has occurred.

FPT_PHP.2.3 For [assignment: *list of TSF devices/elements for which active detection is required*], the TSF shall monitor the devices and elements and notify [assignment: *a designated user or role*] when physical tampering with the TSF's devices or TSF's elements has occurred.

Dependencies: FMT_MOF.1 Management of security functions behaviour

FPT_PHP.3 Resistance to physical attack

Hierarchical to: No other components.

FPT_PHP.3.1 The TSF shall resist [assignment: *physical tampering scenarios*] to the [assignment: *list of TSF devices/elements*] by responding automatically such that the TSP is not violated.

Dependencies: No dependencies

5.1.15 Data Authentication

FDP_DAU.2 Data authentication with identity of guarantor

Hierarchical to: **FDP_DAU.1**

FDP_DAU.2.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of [assignment: *list of objects or information types*].

FDP_DAU.2.2 The TSF shall provide [assignment: *list of subjects*] with the ability to verify evidence of the validity of the indicated information **and the identity of the user that generated the evidence.**

Dependencies: **FIA_UID.1 Timing of identification**

5.1.16 Data exchange integrity

FDP_UIT.1 Data exchange integrity

Hierarchical to: No other components.

FDP_UIT.1.1 The TSF shall enforce the [assignment: *access control SFP(s) and/or information flow control SFP(s)*] to be able to [selection*: transmit, receive*] user data in a manner protected from [selection: *modification, deletion, insertion, replay*] errors.

Dependencies: **[FDP_ACC.1 Subset access control, or**
FDP_IFC.1 Subset information flow control]
[FTP_ITC.1 Inter-TSF trusted channel, or
FTP_TRP.1 Trusted path]

5.1.17 Functions required to support dependencies

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

FDP_ACF.1 Security attribute based access control

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [assignment: *access control SFP*] to objects based on [assignment: *security attributes*, *named groups of security attributes*].

Dependencies: **FDP_ACC.1 Subset access control**
FMT_MSA.3 Static attribute initialisation

FMT_MSA.1 Management of security attributes

Hierarchical to: No other components.

FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to restrict the ability to [selection: *change_default, query, modify, delete,* [assignment: *other operations*]] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

Dependencies: **[FDP_ACC.1 Subset access control or**
FDP_IFC.1 Subset information flow control]
FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MSA.3 Static attribute initialisation

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [selection: *restrictive, permissive, other property*] default values for security attributes that are used to enforce the *SFP*.

FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: **FMT_MSA.1 Management of security attributes**

FMT_SMR.1 Security roles

FDP_IFC.1 Subset information flow control

Hierarchical to: No other components.

FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

Dependencies: **FDP_IFF.1 Simple security attributes**

FMT_MOF.1Management of security functions behaviour

Hierarchical to: No other components.

FMT_MOF.1.1 The TSF shall restrict the ability to [selection: *determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

Dependencies: **FMT_SMF.1 Specification of management functions**
FMT_SMR.1 Security roles

5.2 Operational Security Requirements

5.2.1 Management Functions

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: [assignment: list of security management functions to be provided by the TSF].

Dependencies**: No Dependencies**

<Editor Note: The remaining management functions are extensions to ISO 15408, that is, they are not found in the ISO standard>

MGT_EXT.1 Access revocation

Physical and IT access shall be revoked within [assignment: *time span*] for personnel whose employment or contractual relationship is terminated or for personnel who are temporarily not actively involved in process control and operations (for example, workers on strike, workers on a leave of absence, etc.)

MGT_EXT.2 Backup and Restore

The TSF shall include the capability to backup and restore the system configuration including critical programs, controller instructions and parameters, and instructions and parameters for all sensors and actuators. Backups shall be performed [assignment: frequency] and whenever critical operating parameters [assignment: identify the critical operating parameters] are changed.

MGT_EXT.3 Backup and Restore Self-Testing
The TSF backup and restore procedure shall be able to be self-tested during regular operations and planned maintenance.

5.2.2 Physical Security Requirements

<Editor Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard.>

PHY_EXT.1 Physical Access Control
The TSF shall provide physical access control to critical ICS components including, but not limited to: control room(s), servers, controller, sensors, actuators, and the physical plant under control. <Editor Note: This requirement is included as an example. Physical security requirements should be inserted in this section as appropriate to the specific nature of the target ICS. >

5.3 Integration Security Requirements

5.3.1 Requirements for interfaces between system components

<Editor Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard. >

INT_EXT.1 Authentication Integration
The TSF shall integrate authentication of user access with authentication for physical access such that user access is not granted for a user not identified by the physical access control as being physically present and such that user access is locked when the physical access control indicates that the user is no longer physically present.

5.3.2 Requirements for composability and interoperability between system components

This section documents any requirements specific to security composability that have not been called out as a part of other requirements.

5.3.3 Configuration requirements

<Editor Note: These requirements are extensions to ISO 15408, that is, they are not found in the ISO standard. >

ACM_EXT.1 Configuration Management
The STOE shall be subject to configuration management with an explicit change control and review process.

5.3.4 Integrated assurance requirements

The baseline evaluation assurance level (EAL) for Industrial Control Systems is EAL 3+. The "+" indicates that the EAL is as defined in ISO 15408 Part 3 with additional assurance requirements. In this case the additional requirements reflect the assurances associated with design, development, integration, testing and deployment of a system as opposed to a component or product. In addition, because the ICS is a system, a combination of IT and non-IT security control elements must be considered.

Table 5-1 is the EAL3 summary from ISO 15408, Part 3.

Assurance class	Assurance components
Class ACM: Configuration management	ACM_CAP.3 Authorisation controls
	ACM_SCP.1 TOE CM coverage
Class ADO: Delivery and operation	ADO_DEL.1 Delivery procedures
	ADO_IGS.1 Installation, generation, and start-up procedures
Class ADV: Development	ADV_FSP.1 Informal functional specification
	ADV_HLD.2 Security enforcing high-level design
	ADV_RCR.1 Informal correspondence demonstration
Class AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Class ALC: Life cycle support	ALC_DVS.1 Identification of security measures
Class ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
Class AVA: Vulnerability assessment	AVA_MSU.1 Examination of guidance
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.1 Developer vulnerability analysis

Additional assurance requirements include:

- Formal risk assessment and documentation of an acceptable level of residual risk (note that this is started in this document, the ICS-SPP and further refined in the subsequent elaboration of this SPP into an SPP for a specific system or into a system security target (SST) for a specific system)
- Periodic risk management including, as a minimum,
    - Periodic reassessment of risk

    - Periodic vulnerability assessment
- Interoperability testing
- Deployment testing

<Editor Note: The above outlines extensions to assurance requirements that will be more fully developed.>

The general intent of the assurance requirements and associated system evaluation activities is to confirm that the acceptable level of residual risk as documented in the SPP is achieved in the operational system.

6 Application Notes

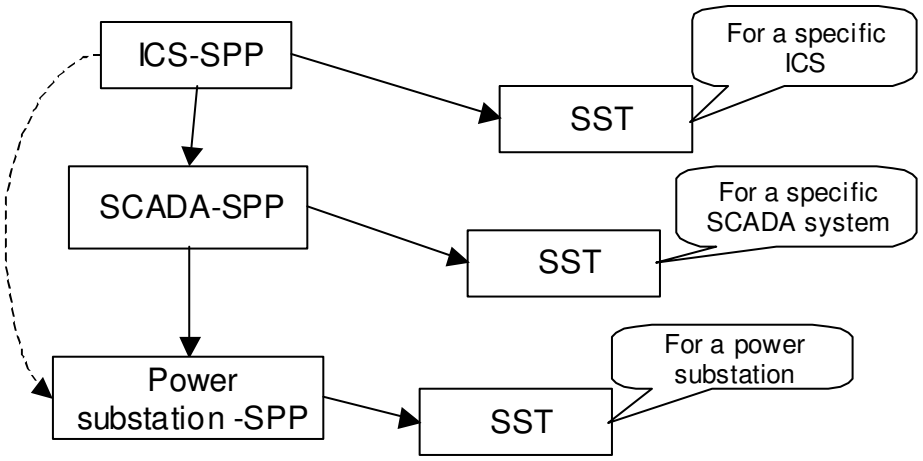
This section of the document contains supporting information that will be useful in developing more focused system protection profiles or security targets for specific classes of industrial control systems, for example SCADA systems, or for specific applications of industrial control systems.

The intended relationship of this baseline IC-SPP to other system protection profiles, functional packages, assurance packages, system security targets and industry specific instantiations of each:

A system protection profile provides a statement of the security requirements, generally at an abstract / implementation independent level but can provide industry specific implementation details to ensure consistent compliance.

Therefore, for a specific community of interest (e.g. the process control industry) providing a related family of “constructs” (i.e. system protection profiles, functional packages, assurance packages, system security targets) that help to ensure interoperability, provide for a consistent implementation of security controls, countermeasures and ensures sufficient assurance (confidence in the ultimate system).

The following diagram illustrates how the Application Notes will eventually provide the required guidance on how to develop, and the relationships amongst the family of “constructs” being developed to support the ICS.



Relationship between ICS-SPP and other potential SPP's and SST's

7 Rationale

This section presents the evidence used in evaluation of this system protection profile. The evidence supports the claims that the SPP is a complete and cohesive set of requirements and that a conformant system TOE would provide an effective set of IT and operational security countermeasures to the defined set of threats.

7.1 Security objectives rationale

This section of the document demonstrates that the stated security objectives are traceable to all of the aspects identified in the STOE security environment and are suitable to cover them.

The following table documents summarizes the security objectives rationale. The table shows the association of security objectives with threats and impacts (if the threat is successfully realized) to each set of critical assets.

<Editor Note: The reconciliation of this table with the defined security objectives is incomplete.>

Asset	Threat	Impact	Security Objectives	
Sensors and Actuators	Unauthorized changes are made to set points, calibrations or other critical device settings	- Loss of control of the process - Possible failure of safety system	Preventive	O2.1 O6.1 O5.1s
			Detective	
			Corrective	O4.1

Asset	Threat	Impact	Security Objectives	
	Sensors or actuators are physically tampered with	- Loss of control of the process - Possible shutdown of process - Possible failure of safety system	Preventive	O1.2
			Detective	
			Corrective	
	Sensors or actuators are disabled (for example via exploitation of vulnerabilities such as malformed packets or buffer overflows)	- Loss of control of the process - Possible shutdown of process - Possible failure of safety system	Preventive	Vulnerability testing of system components O1.1 O2.1 O1.2
			Detective	
			Corrective	O4.1
Controllers	Unauthorized changes are made to programmed instructions	- Loss of control system integrity leading to disruption of operations	Preventive	O2.1 O1.1
			Detective	Audit logical access to controllers Audit physical access to controllers
			Corrective	O4.1
	Controllers are disabled (for example via exploitation of vulnerabilities such as malformed packets or buffer overflows)	- Loss of process control - Possible damage to equipment - Possible failure of safety system	Preventive	O1.1 O1.2
			Detective	Audit logical access to controllers Audit physical access to controllers
			Corrective	
HMI's	Unauthorized changes are made	- Loss of operator control	Preventive	O1.1 O1.2

Asset	Threat	Impact	Security Objectives	
	to alarm thresholds or other critical operator information displays	- Possible damage to equipment - Possible failure of safety system	Detective	Audit HMI changes
			Corrective	O4.1
The controlled process	The power supply to the industrial control system is disrupted	- The ICS fails causing disruption of the controlled process	Preventive	OE1.1
			Detective	
			Corrective	O4.1
	Interference with operation of safety systems	- The control system is forced into safety override mode reducing or eliminating security controls	Preventive	O1.2 O1.1
			Detective	Audit safety system activity
			Corrective	
Process control signals, data and information	Data is tapped on a process control data communications line	Data may be captured by for later use in a replay attack or other attack	Preventive	O1.2 Prevent data disclosure, detect tampering
			Detective	Detect data tampering
			Corrective	
	False information is sent to control system operators	- Operators cannot see true process state and lose control of the process - Possible masking of other malicious activity - Operators may initiate inappropriate action	Preventive	O1.1 O1.2
			Detective	Authenticate data within process control network (detect data tampering) O2.1
			Corrective	O4.1
	False control or sensor signals are	- Loss of operator control of the process	Preventive	O1.1 O1.2

Asset	Threat	Impact	Security Objectives	
	sent to controllers and/or actuators		Detective	O5.1 O3.1, O2.1
			Corrective	
Process control business or financial information	False business or financial information is sent from the control system to business systems	- Theft or diversion of resources masked - Business operations disrupted	Preventive	O1.1
			Detective	O2.1 O5.1, O5.2 Audit use of program generating business data
			Corrective	

7.2 Security requirements rationale

1020 This section of the document demonstrates that the combined set of all the security requirements types, IT, operational and integration, for the TOE and the environment meet and are traceable to the security objectives.